Innovative cryptographic approaches to computer systems security

博士学位論文
論文内容の要旨および審査結果の要旨

論文題目	Innovative cryptographic approaches to computer systems security
氏　　名	OGIELA, Urszula
学位の種類	博士（工学）
学位授与年月日	2019 年 3 月 24 日
学位授与の条件	法政大学学位規則第 5 条第 1 項第 2 号該当者（乙）
論文審査委員	主　査　滝沢　誠　教授
	副　査　三浦　孝夫　教授
	副　査　塩谷　勇　教授
	副　査　BAROLLI, Leonard　教授（福岡工業大学）

2019年 1月 24日

学位論文審査委員会

委員長　藤井章博　殿

学位論文審査小委員会

主査　教授 滝沢武 印

副査　教授 三輪洋文 印

副査　教授 塩谷勇 印

副査　教授 BAROLLI LEONARD 印

試問による学識確認の報告

法政大学学位規則第２０条により、OGIELA, Urszula 氏について、その論文を中心に関連する学問領域の試問を行った結果、合格と判定した。

以　上

（報告様式Ｉ・論文博士）

2019 年　1 月 24 日

学位論文審査委員会

委員長　藤井章博　殿

学位論文審査小委員会

主査　教授 滝沢武 ㊞

副査　教授 三浦孝夫 ㊞

副査　教授 塩谷勇 ㊞

副査　教授 BAROLLI LEONARD ㊞

OGIELA, Urszula 氏　提出学位請求論文

「Innovative cryptographic approaches to computer systems security」

論文内容の要旨と審査結果の要旨（報告）

（報告様式Ⅱ）

１．論文内容の要旨

本論文「Innovative cryptographic approaches to computer systems security」では、情報システムのセキュリティを保持するための秘密情報分散、共有法を、言語学的(linguistic)な方法論に生体情報を用いた(biometric)方法論を組み合わせた新しい方法論により取り組んだ研究についてまとめられている。秘密分散共有法の(n, m)閾値法は、著名な Adi Shamir により提起されたもので、秘密情報 S を n 個の部分(shadow)に分割し、この中の任意の m 個の部分により秘密情報 S を復元できるが、m 個より少ない部分では復元できないようにする方法である。本研究では、従来の(n, m)閾値法を、まず言語学的に考察し、新たに文脈自由文法により、秘密情報を n 個の部分に分割、共有する言語学的閾値法(linguistic threshold scheme)を提案している。さらに、分割された n 個の部分に対して、DNA 情報等の生体情報を与える生体情報閾値法(biometric threshold scheme)を新たに提案している。従来の秘密情報分割共有法では、共有される秘密情報と、秘密情報の所有者個人との関連性は議論されてきていなかった。本論文で新たに提案されている言語学的、生体情報閾値法(linguistic-biometric threshold scheme)では、各個人固有の秘密情報を n 個の部分に分割、生成するための言語学的(linguistic)閾値法、秘密情報の所有者を特定するための生体情報閾値法を融合したものである。本閾値法により、分割された秘密情報の部分から、元の秘密情報を復元できると同時に、情報の所有者を識別することが可能となるもので、この点に、新規性と有用性があるものである。

本論文の構成は以下のようである。

第 1 章では、コンピュータ科学分野の中で暗号化研究についての動向を述べ、本論文の目的、議論すべき問題点を論じている。また、本論文の構成と各章の概要を述べている。

第 2 章では、情報セキュリティを考えるときに基礎となる概念、理論、アルゴリズムについて述べている。特に、A. Shamir により提起された古典的な秘密情報分割、復元理論による(n, m)閾値法について論じている。

第 3 章では、言語学的(linguistic)方法論による言語学的閾値法(linguistic threshold scheme)を新たに提案している。特に、文脈自由文法を用いて、秘密情報を n 個の部分(shadow)に分割する閾値法を新たに提案している。

第 4 章では、生体情報を用いた閾値法(biometric threshold scheme)を新たに提案している。(n,m)閾値法により秘密情報を n 個の部分(shadow)に分割するが、分割された秘密情報部分に、個人の DNA、指紋等の生体情報を与える方法を新たに提案している。これにより、秘密情報の所有者を識別することが可能となるものである。各種の生体情報の符号化についても論じている。

第 5 章では、これまでの議論に基づいて、情報システムを安全(secure)にするためのプロトコルについて論じている。本論文で議論してきた言語学的かつ生体情報を用いた閾値法の評価を行っている。システムの実装を行い、特に、クラウドコンピューティングシステ

ムを対象として、大規模な情報システムを階層化するときの秘密情報共有、個人認証のためのモデルを示し、CAPTCHA について実験を行い、本閾値法の有用性を示している。

第 6 章では、本論文の意義、成果のまとめを行なっている。また、今後の研究の方向性について論じている。

2．審査結果の要旨

本論文は、これまで多くの研究が進められてきている記号についての秘密情報分割、共有化のための閾値法に対して、指紋、DNA 等の個人の生体情報を融合する新しい方法論を提案している。本論文の第 3 章では、文脈自由文法を用いた言語学的閾値法を新たに提案している。第 4 章では、生体情報により、秘密情報に生体情報を与えることにより、秘密情報の秘密性のみならず秘密情報の所有者の特定を可能とする閾値法を提案している。第 5 章は、本論文の核となるもので、言語学的閾値法と生体情報閾値法を融合化したプロトコル、アルゴリズムを提案し、実装し実験により評価を行い本方法論の有用性を示している。

本論文は、言語学的な記号論に基づいた暗号化と生体情報にもとづいた暗号化を融合するためのモデル、アルゴリズムを新たに示している点に、新規性と有用性がある。これらの方法論は、生体情報を含めた情報科学の境界領域の研究としても重要である。本論文による成果は、理工学的に新規性がありかつ有用なもので、次世代の情報システムを考えるときに新しい方法論、知見を与えるものである。

これまでに、本論文に関連した論文として、2009 年以降に国際学術論文誌に 10 件(筆頭著者論文 3 件)を論文として発表している。本論文は、これらの研究成果を整理し体系化しまとめたものである。これらの国際学術論文誌論文に加えて、国際会議で 27 件(査読付き)、著書 6 件を発表している。さらに、国際会議 AIT-2010 では、Best paper 賞を受賞する等、国際的にも高い評価を得てきている。

よて、本審査小委員会は、全会一致をもって、提出論文が博士（工学）の学位に値するという結論に達した。